MONTANA CHEMICAL DEPENDENCY CENTER POLICY AND PROCEDURE MANUAL

Policy Subject: Network & File Server Security	
Policy Number: CUP 11	**Standards/Statutes: ARM 37.27.120**
Effective Date: 01/01/02	**Page 1 of 3**

PURPOSE:
Physical and administrative access to the state network must be controlled to prevent the intentional or unintentional modification, destruction, disclosure, or misuse of data and information resources.

POLICY:

The State provided Network and File Server services are to be used for: the conduct of State and local government business and delivery of government services; transmitting and sharing of information among governmental, research, and educational organizations; supporting open research and education in and between national and international research and instructional institutions; communicating and exchanging professional information; encouraging debate of issues in a specific field of expertise; applying for or administering grants or contracts; announcing requests for proposals and bids; announcing new services for use in research or instruction; and conducting other appropriate State business.

PROCEDURE:

PHYSICAL ACCESS - Only personnel authorized to operate a file server will have access to the physical area where the file server resides. Keys and/or other security devices must be used to secure the physical area and a list of all authorized personnel maintained. In areas with highly secure file servers, an authorized user must supervise cleaning and maintenance personnel while they are working in the area.

ADMINISTRATIVE ACCESS - Supervisor level access given to employees must be approved by the Director or the Information Systems Technician. Employees having user IDs with Supervisor privileges will be documented including the need for Supervisor access. User D's with Supervisor level access must follow state policy regarding passwords. Information Systems Technicians must use the Supervisor user ID only when doing system administration or troubleshooting. A second user ID with standard privilege levels must be used for day-to-day activities.

AUDIT LOG REQUIREMENTS - The use of Supervisor User ID's must be logged using either an access log or an auditing software package. Anytime "CONSOLE" or
Administrative access is gained to an agency server, it must be logged in an access log containing the date, time, network address, user, and a description of what was done and why. Agencies must be notified when anyone outside the agency gains console or administrative access to one of their file servers.

Computer systems handling sensitive, valuable, or critical information must log all significant computer security relevant events. Examples of computer security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, modifications to system software, and administration changes affecting the state network. Designated Agency Security Officers will administer auditing functions. Periodic checks of auditing logs must be completed. Any security violations must be reported to the Information Systems Technician.

Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, security measures. These logs must be retained for at least five (5) years.

Exceptions to this policy must be documented by the Information Systems Technician and approved by the State Security Officer.

It is recommended that physical access to file servers in a peer-to-peer environment is controlled, but due to the fact these computers may be used as workstations, it is not required.

File servers and other network equipment should be kept in a no-traffic locked room. The room should withstand hazards such as fire, flooding and natural disasters. The room's heat, ventilation and air conditioning (HVAC) systems should be reliable. Electrical power should be reliable and all critical electronic devices should be powered through un-interruptible power supplies (UPS) correctly sized for running the devices long enough for an automated or manual shutdown of the device.

Access to network equipment such as hubs, MAUs, routers, bridges, patch panels, gateways, communication servers and the like should be controlled the same as file servers. Physical access should be restricted to prevent tampering or accidental disruption of service.

The server console or access to administrative areas on the file server should be password protected. Computer systems should be periodically audited for compliance with the existing security policies. These audits should be performed at least once a quarter.

Revisions:

Prepared By: Rona McOmber Information System Technician 10/30/01
Name Title Date

Approved By: 01/01/02
David J. Peshek, Administrator